REMARKS

General Matters

Applicant thanks the Examiner for acknowledging Applicant's claim to foreign priority and receipt of the certified copy of the priority document. Further, Applicant thanks the Examiner for considering two of the three references cited in the Information Disclosure Statement filed on April 29, 2004. However, it does not appear that the Examiner has indicated that reference Sangyo Tosyo Shuppan, "Modern Cryptography", July 30, 1997, pages 131-150, has been considered. In the second paragraph of page 2 the Information Disclosure Statement, Applicant indicated that the concise explanation required for foreign language documents was complied with through discussion of the reference in the specification at page 2, line 6. Applicant has thus complied with the requirements for submission of non-English language references, as required by MPEP § 609.04(a)(III), and Applicant respectfully requests the Examiner to indicate consideration of this reference in the next office communication.

Furthermore, Applicant notes that the Office Action Summary did not indicate acceptance of the drawings. Applicant respectfully requests the Examiner to indicate acceptance of the drawings in the next office communication.

Status of the Application

Claims 1-11 are all the claims pending in the application. Claims 1-11 are rejected as allegedly being unpatentable on the ground of nonstatutory obviousness-type double patenting over claims 1-53 of Furukawa, et al. (U.S. Patent No. 7,003,541 B2, hereinafter "the '541 patent") and also over claims 1-18 of Furukawa, et al (U.S. Patent No. 7,035,404 hereinafter "the '404 patent"). Further, claims 1-11 are rejected under 35 U.S.C. § 102(b) as being anticipated by

Kanda, et al. (U.S. Patent No. 6,011,848). Applicant here responds to each grounds of rejection and respectfully requests favorable reconsideration.

Nonstatutory Obviousness Type Double Patenting Rejection

As MPEP § 804 explains, the "analysis employed in an obviousness-type double patenting rejection parallels the guidelines for analysis of a 35 U.S.C. 103 obviousness determination." MPEP § 804 further explains that

> Any obviousness-type double patenting rejection should make clear:
>
> (A) The differences between the inventions defined by the conflicting claims - a claim in the patent compared to a claim in the application; and
>
> (B) The reasons why a person of ordinary skill in the art would conclude that the invention defined in the claim at issue is anticipated by, or would have been an obvious variation of the invention defined in a claim in the patent.

The grounds of rejection for rejecting both the '541 and the '404 patents do not fulfill this requirement. The grounds of rejection do not effectively point to differences in the conflicting claims. In both nonstatutory double patenting rejections, the grounds of rejection cite the claim language of claim 1 almost in its entirety and asserts that it "is referred to in the patent claims as" a portion of claim 1 from each patent. In both cases, the grounds of rejection assert that "the patent claims contain all the limitations of the instant application," but there is no indication in the Office Action where the various elements of the present claims are to be found in the cited portions of the patent claims, or where the claims differ. The grounds of rejection also fail to give reasons why a person of ordinary skill in the art would conclude that the inventions defined in the claims at issue would have been anticipated by or obvious over the invention defined in claims of either patent. The grounds of rejection thus fail to present a *prima facie* case of obviousness type double patenting and also fail to follow the guidelines of the MPEP.

Furthermore, contrary to the assertion in the Office Action, the claims of the present application are not anticipated by the claims of either the Furukawa '541 patent or the Furukawa '404 patent, since neither the '541 nor the '404 patents disclose all the limitations recited in claims of the present application in as complete detail as recited in claims 1-11 of the present application. The grounds of rejection do not point out individually where any of the elements of the present claims are to be found in the cited patent claims, and it is respectfully submitted that many of the elements of the present claims are not recited in the claims of the cited patents. For example, present claim 1 recites a generator that supplies the common input to the prover, the verifier, the simulator and the distinguisher, and supplies the witness to the prover and the distinguisher. This element is not recited by the claims of the '541 patent or the '404 patent. Also, present claim 1 recites a proof history and a simulated proof history, neither of which is found in the claims of the '541 patent or the '404 patent. Not only do the '541 and the '404 patents not recite these elements, it is respectfully submitted that it would not have been obvious to have included those features in the '541 and '404 claims. Applicant thus respectfully requests that the Examiner withdraw the obviousness-type double patenting rejection over both the '541 and the '404 patent.

Rejection Under 35 U.S.C. § 102(b)

Claims 1-11 are rejected under 35 U.S.C. § 102(b) for allegedly being anticipated by Kanda, et al. (U.S. Patent No. 6,011,848). Applicant respectfully traverses this rejection.

Claim 1 recites a prover, a verifier, a generator, a simulator, and a distinguisher. The grounds of rejection fail to particularly point out which section or embodiment of Kanda corresponds to each of these elements recited in claim 1. For example, claim 1 recites, inter alia, a generator that supplies the common input to the prover, the verifier, the simulator, and the distinguisher, and supplies the witness to the prover and the distinguisher. No such element is taught or suggested in Kanda. In particular, the cited passage (col. 6, line 21 - col. 8, line 41) fails to teach or suggest this element.

Claim 1 further recites a proof history and simulated proof history. Kanda discloses neither. Claim 1 also recites that the distinguisher evaluates the proof system depending on whether a difference in distribution between the proof history and the simulated proof history is computationally indistinguishable for a great majority of possible common inputs and computationally distinguishable for at least one of the possible common inputs, which Kanda does not disclose.

As these examples demonstrate, Kanda does not reveal most of what is recited in claim 1, and the grounds of rejection do not indicate where any of the individual elements of claim 1 are disclosed in Kanda. Applicant therefore respectfully submits that claim 1 is patentable over Kanda at least due to these deficiencies, as well as other recited features of claim 1. Furthermore, claims 2-6 are also patentable over Kanda at least due to their dependence from claim 1, as well as their other recited features.

Further with respect to claim 6, in addition to evaluating a proof system, claim 6 recites that "the evaluation result stored in the memory is accessible through a network." For example, as shown in one exemplary embodiment in Fig. 6, when it receives a request from a user terminal 1007 through a network 1008, a provider terminal 1003 responsively transmits necessary information, such as the evaluation result and the evaluation material, to the user terminal 1007 through the network 1008. No such feature is disclosed in Kanda. Indeed, Kanda does not disclose that "the distinguisher evaluates the proof system depending on whether a difference in distribution between the proof history and the simulated proof history is computationally indistinguishable for a great majority of possible common inputs and computationally distinguishable for at least one of the possible common inputs", as recited in claim 1, and therefore does not produce the "evaluation result" recited in claim 6. Furthermore, the system recited in claim 1 (and which is not disclosed by Kanda) allows the evaluation result to have "zero-knowledge", as explained in the background section and exemplary embodiments of the present invention as described in the specification. This enables the evaluation result to be "on public view", as recited in claim 5, and "accessible through a network", as recited in claim 6. No similar evaluation result is disclosed as being produced by the system of Kanda.

Claims 7-11 also recite various elements addressed above that are not taught or suggested by Kanda. Kanda does not disclose most of the elements of claims 7-11, and the grounds of rejection fail to point out where Kanda teaches or suggests the individual elements of claims 7-11. For example, claim 7 recites supplying the common input to the prover, the verifier, the simulator, and the distinguisher, and supplying the witness to the prover and the distinguisher. Kanda does not teach or suggest most of these elements. Applicant respectfully submits that claim 7 is patentable over Kanda at least for these reasons, as well as other recited features.

Claims 8 and 10, in addition to reciting some of the elements addressed above, also recite a common input comprising g, h, $y=g^2$, and z' and a witness comprising x from the third random tape, wherein x is an integer and g, h, and z' are elements of a group which is previously determined and has an order thereof. Kanda fails to disclose such a common input. Claims 8 and 10 further recite that the prover uses the first random tape to uniformly and randomly select d,e, and f, which are integers smaller than the order of the group, and calcultates $h'=h^d$, $w'=z'^d$,

$v=h^{xd}$, $y'=g^{e}$, $v'=h'^{e}$, h'',h^{f}, and $w''=z'^{f}$. This is not taught or suggested by Kanda. Applicant therefore respectfully submits that claims 8 and 10 are patentable over Kanda at least due to these distinctions, as well as other recited features of claims 8 and 10.

Claim 9 recites a prover having a first random tape, a verifier having a second random tape, and a third random tape; this is not taught or suggested by Kanda. Claim 9 further recites generating a proof history and generating a simulated proof history, which is not taught or suggested by Kanda. Applicant therefore respectfully submits that claim 9 is patentable over Kanda at least for these reasons, as well as other features recited in claim 9.

Claim 11 recites that a proof history is generated and a simulated proof history is generated; Kanda does not teach or suggest this. Applicant therefore respectfully submits that claim 11 is patentable over Kanda at least for these reasons, as well as other features recited in claim 11.

Applicant therefore respectfully requests that the rejection under 35 U.S.C. § 102(b) over Kanda be withdrawn.

Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880 via EFS payment screen. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

for/ Reg.# 39,283
Howard L. Bernstein
Registration No. 25,665

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: March 10, 2008